BUNDESREPUBLIK DEUTSCHLAND

Bescheinigung

Die Giesecke & Devrient GmbH in München/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Zugriffsgeschützter Datenträger"

am 18. Mai 1998 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig das Symbol G 06 K 19/073 der Internationalen Patentklassifikation erhalten.

München, den 21. Juni 1999
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Ebert

Aktenzeichen: 198 22 217.3

Zugriffsgeschützter Datenträger

Die Erfindung betrifft einen Datenträger, der einen Halbleiterchip aufweist, in dem geheime Daten abgespeichert sind. Insbesondere betrifft die Erfindung eine Chipkarte.

Datenträger die einen Chip enthalten, werden in einer Vielzahl von unterschiedlichen Anwendungen eingesetzt, beispielsweise zum Durchführen von Finanztransaktionen, zum Bezahlen von Waren oder Dienstleistungen, oder als Identifikationsmittel zur Steuerung von Zugangs- oder Zutrittskontrollen. Bei allen diesen Anwendungen werden innerhalb des Chips des Datenträgers in der Regel geheime Daten verarbeitet, die vor dem Zugriff durch unberechtigte Dritte geschützt werden müssen. Dieser Schutz wird unter anderem dadurch gewährleistet, daß die inneren Strukturen des Chips sehr kleine Abmessungen aufweisen und daher ein Zugriff auf diese Strukturen mit dem Ziel, Daten, die in diesen Strukturen verarbeitet werden, auszuspähen, sehr schwierig ist. Um einen Zugriff weiter zu erschweren, kann der Chip in eine sehr fest haftende Masse eingebettet werden, bei deren gewaltsamer Entfernung das Halbleiterplättchen zerstört wird oder zumindest die darin gespeicherten geheimen Daten vernichtet werden. Ebenso ist es auch möglich, das Halbleiterplättchen bereits bei dessen Herstellung mit einer Schutzschicht zu versehen, die nicht ohne Zerstörung des Halbleiterplättchens entfernt werden kann.

Mit einer entsprechenden technischen Ausrüstung, die zwar extrem teuer aber dennoch prinzipiell verfügbar ist, könnte es einem Angreifer möglicherweise gelingen, die innere Struktur des Chips freizulegen und zu untersuchen. Das Freilegen könnte beispielsweise durch spezielle Ätzverfahren

oder durch einen geeigneten Abschleifprozeß erfolgen. Die so freigelegten Strukturen des Chips, wie beispielsweise Leiterbahnen, könnten mit Mikrosonden kontaktiert oder mit anderen Verfahren untersucht werden, um die Signalverläufe in diesen Strukturen zu ermitteln. Anschließend könnte versucht werden, aus den detektierten Signalen geheime Daten des Datenträgers, wie z.B. geheime Schlüssel zu ermitteln, um diese für Manipulationszwecke einzusetzen. Ebenso könnte versucht werden, über die Mikrosonden die Signalverläufe in den freigelegten Strukturen gezielt zu beeinflussen.

Der Erfindung liegt die Aufgabe zugrunde, geheime Daten, die in dem Chip eines Datenträgers vorhanden sind, vor unberechtigtem Zugriff zu schützen.

Diese Aufgabe wird durch die Merkmalskombination des Anspruchs 1 gelöst.

Bei der erfindungsgemäßen Lösung werden im Gegensatz zum Stand der Technik keine Maßnahmen getroffen, um ein Freilegen der internen Strukturen des Chips und ein Anbringen von Mikrosonden zu verhindern. Es werden stattdessen Maßnahmen getroffen, die es einem potientellen Angreifer erschweren, aus den gegebenenfalls abgehörten Signalverläufen Rückschlüsse auf geheime Informationen zu schließen. Diese Maßnahmen bestehen erfindungsgemäß darin, sicherheitsrelevante Operationen nicht mit echten Geheimdaten durchzuführen, sondern mit verfälschten Geheimdaten, aus denen die echten Geheimdaten nicht ohne Hinzunahme weiterer geheimer Informationen ermittelbar sind. Dies hat zur Folge, daß ein Angreifer selbst dann, wenn es ihm gelungen ist, die bei einer Operation verwendeten Geheimdaten zu ermitteln, damit keinen Schaden anrichten kann, da es sich bei den ausgespähten Daten nicht um die echten Geheimdaten sondern um verfälschte Geheimdaten handelt.

Um die Funktionsweise des Datenträgers zu gewährleisten, muß sichergestellt sein, daß der Datenträger bei rechtmäßiger Verwendung trotz der verfälschten Geheimdaten die richtigen Ergebnisse liefert. Dies wird dadurch erreicht, daß zunächst eine Funktion festgelegt wird, mit der die echten Geheimdaten verfälscht werden, beispielsweise eine EXOR-Verknüpfung der Geheimdaten mit einer Zufallszahl. Die echten Geheimdaten werden mit der so festgelegten Funktion verfälscht. Mit den verfälschten Geheimdaten werden all diejenigen Operationen im Datenträger durchgeführt, bei denen die Verfälschung der Geheimdaten anschließend wieder kompensiert werden kann. Im Falle von EXOR-verfälschten Geheimdaten wären das Operationen, die bezüglich EXOR-Verknüpfungen linear sind. Bevor eine Operation ausgeführt wird, die eine derartige Kompensation nicht zuläßt, beispielsweise eine bezüglich EXOR-Verknüpfung nichtlineare Operation, müssen die echten Geheimdaten wiederhergestellt werden, so daß diese Operation mit den echten Geheimdaten ausgeführt wird. Die Wiederherstellung der echten Geheimdaten nach Durchführung einer kompensierbaren Funktion erfolgt beispielsweise dadurch, daß der mittels der verfälschten Geheimdaten ermittelte Funktionswert mit einem entsprechenden Funktionswert der für die Verfälschung verwendeten Zufallszahl EXOR verknüpft wird. In diesem Zusammenhang ist es wichtig, daß Zufallszahl und Funktionswert vorab in einer sicheren Umgebung ermittelt und gespeichert wurden, damit die Berechnung des Funktionswerts aus der Zufallszahl nicht abgehört werden kann.

Die obige Vorgehensweise hat zur Folge, daß die echten Geheimdaten nur für die Durchführung von den Operationen, wie z.B. nichtlineare Operationen verwendet werden, für die dies unbedingt erforderlich ist, d.h. die nicht ersatzweise mit verfälschten Geheimdaten durchgeführt werden können. Da

derartige Operationen in der Regel sehr komplex und nicht einfach analysierbar sind, ist es für einen potentiellen Angreifer extrem schwierig wenn nicht sogar unmöglich, aus einer Analyse der von diesen Operationen hervorgerufenen Signalverläufe die echten Geheimdaten in Erfahrung zu bringen. Da die einfachen strukturierten Funktionen, bei denen eine nachträgliche Kompensation derVerfälschung möglich ist, mit verfälschten Geheimdaten durchgeführt werden, wird es durch die beschriebene Vorgehensweise extrem erschwert, aus unberechtigt abgehörten Signalverläufen die echten Geheimdaten des Datenträgers zu ermitteln.

Die Erfindung wird nachstehend anhand der in den Figuren dargestellten Ausführungsformen erläutert. Es zeigen:

Fig. 1 eine Chipkarte in Aufsicht,

Fig. 2 einen stark vergrößerten Ausschnitt des Chips der in Fig. 1 dargestellten Chipkarte in Aufsicht,

Fig. 3 eine schematische Darstellung eines Ausschnitts aus einem Funktionsablauf innerhalb der Chipkarte und

Fig. 4 eine Variante zu dem in Fig. 3 dargestellten Funktionsablauf.

In Fig. 1 ist als ein Beispiel für den Datenträger eine Chipkarte 1 dargestellt. Die Chipkarte 1 setzt sich aus einem Kartenkörper 2 und einem Chipmodul 3 zusammen, das in eine dafür vorgesehene Aussparung des Kartenkörpers 2 eingelassen ist. Wesentliche Bestandteile des Chipmoduls 3 sind Kontaktflächen 4, über die eine elektrische Verbindung zu einem externen Gerät hergestellt werden kann und ein Chip 5, der mit den Kontaktflächen 4 elektrisch

verbunden ist. Alternativ oder zusätzlich zu den Kontaktflächen 4 kann auch eine in Fig. 1 nicht dargestellte Spule oder ein anderes Übertragungmittel zur Herstellung einer Kommunikationsverbindung zwischen dem Chip 5 und einem externen Gerät vorhanden sein.

In Fig. 2 ist ein stark vergrößerter Ausschnitt des Chips 5 aus Fig. 1 in Aufsicht dargestellt. Das besondere der Fig. 2 liegt darin, daß die aktive Oberfläche des Chips 5 dargestellt ist, d.h. sämtliche Schichten, die im allgemeinen die aktive Schicht des Chips 5 schützen, sind in Fig. 2 nicht dargestellt. Um Informationen über die Signalverläufe im Inneren des Chips zu erhalten, können beispielsweise die freigelegten Strukturen 6 mit Mikrosonden kontaktiert werden. Bei den Mikrosonden handelt es sich um sehr dünne Nadeln, die mittels einer Präzisions-Positioniereinrichtung mit den freigelegten Strukturen 6, beispielsweise Leiterbahnen in elektrischen Kontakt gebracht werden. Die mit den Mikrosonden aufgenommenen Signalverläufe werden mit geeigneten Meß- und Auswerteeinrichtungen weiterverarbeitet mit dem Ziel, Rückschlüsse auf geheime Daten des Chips schließen zu können.

Mit der Erfindung wird erreicht, daß ein Angreifer auch dann, wenn es ihm gelungen sein sollte, die Schutzschicht des Chips 5 ohne Zerstörung des Schaltkreises zu entfernen und die freigelegten Strukturen 6 des Chips 5 mit Mikrosonden zu kontaktieren oder auf andere Weise abzuhören nur sehr schwer oder gar nicht Zugang zu insbesondere geheimen Daten des Chips erlangt. Selbstverständlich greift die Erfindung auch dann, wenn ein Angreifer auf andere Art und Weise Zugang zu den Signalverläufen des Chips 5 erlangt.

Fig. 3 zeigt eine schematische Darstellung eines Ausschnitts aus einem Funktionsablauf in der Chipkarte. Für die Darstellung wurde beispielhaft

eine Verschlüsselungsoperation ausgewählt. Die an diesem Beispiel erläuterten Prinzipien sind aber auch für beliebige andere sicherheitsrelevante Operationen anwendbar. Zu Beginn des in Fig. 3 dargestellten Ausschnitts der Verschlüsselungsoperation werden Daten abc, die im Klartext oder bereits verschlüsselt vorliegen können, einem Verknüpfungspunkt 7 zugeführt. Im Verknüpfungspunkt 7 findet eine Verknüpfung der Daten abc mit einem Schlüssel K1 statt. Im vorliegenden Beispiel handelt es sich bei dieser Verknüpfung um eine EXOR-Verknüpfung, es können jedoch auch andere geeignete Verknüpfungsformen eingesetzt werden. Auf das Verknüpfungsergebnis wird daraufhin in einem Funktionsblock 8 eine nichtlineare Funktion g angewendet. Um darzustellen, daß der Funktionsblock 8 eine nichtlineare Funktion repräsentiert, ist dieser in Fig. 3 in Form eines verzerrten Rechtecks abgebildet. Die mit dem Funktionsblock 8 erzeugten Daten werden in einem Verknüpfungspunkt 9 mit einer Zufallszahl Z EXOR verknüpft und anschließend in einem Funktionsblock 10 weiterverarbeitet. Durch die Verknüpfung mit der Zufallszahl Z findet eine Verfälschung der Daten statt, die einem Angreifer eine Analyse der Vorgänge im Funktionsblock 10, der eine lineare Abbildung mittels einer Funktion f repräsentiert, erschwert. Als Symbol für eine lineare Funktion wird in Fig. 3 ein unverzerrtes Rechteck verwendet. Die im Funktionsblock 10 erzeugten Daten werden in einem Verknüpfungspunkt 11 mit Daten f (Z) verknüpft, die vorab z.B. bei der Herstellung der Karte durch Anwendung der Funktion f auf die Zufallszahl Z erzeugt wurden. Durch diese Verknüpfung wird die Verfälschung der Daten mit der Zufallszahl Z im Verknüpfungspunkt 9 kompensiert. Diese Kompensation ist erforderlich, da anschließend die nichtlineare Funktion g im Funktionsblock 12 auf die Daten angewendet werden soll und nach Anwendung einer nichtlinearen Funktion auf die Daten eine Kompensation der Verfälschung nicht mehr möglich ist. Weiterhin werden die Daten im Verknüp-

fungspunkt 11 mit einem Schlüssel K2 EXOR-verknüpft, der im Rahmen der Verschlüsselungsoperation erforderlich ist.

Die Verknüpfung im Verknüpfungspunkt 11 mit den Daten f (Z) und K2 kann entweder mit den Einzelkomponenten K2 und f (Z) erfolgen oder mit dem Ergebnis einer EXOR-Verknüpfung dieser Einzelkomponenten. Letztere Vorgehensweise eröffnet die Möglichkeit, daß der Schlüssel K2 nicht im Klartext verfügbar sein muß sondern lediglich der mit f (Z) EXOR-verknüpfte Schlüssel K2. Wenn dieser Verknüpfungswert bereits vorab, z.B. während der Initialisierung oder Personalisierung der Chipkarte 1 berechnet wurde und im Speicher der Karte abgespeichert wurde, ist es nicht erforderlich, den Schlüssel K2 im Klartext in der Chipkarte 1 zu speichern. Auf diese Art und Weise kann die Sicherheit der Chipkarte 1 weiter erhöht werden.

Nach Anwendung der Funktion g auf die Daten im Funktionsblock 12 wird das so ermittelte Ergebnis in einem Verknüpfungspunkt 13 wiederum mit der Zufallszahl Z verknüpft und damit verfälscht. Es folgt im Funktionsblock 14 wiederum eine Anwendung der linearen Funktion f auf das Verknüpfungsergebnis. Schließlich findet an einem Verknüpfungspunkt 15 eine EXOR-Verknüpfung der Daten mit dem Ergebnis einer Anwendung der Funktion f auf die Zufallszahl Z statt und mit einem Schlüssel K3. An diese Verknüpfung können sich weitere Verarbeitungsschritte anschließen, die in Fig. 3 jedoch nicht dargestellt sind.

Insgesamt kann die in Fig. 3 dargestellte Vorgehensweise so zusammengefaßt werden, daß die in der Verschlüsselungsoperation verarbeiteten Daten immer dann, wenn dies möglich ist, durch EXOR-Verknüpfung mit einer Zufallszahl Z verfälscht werden, um ein Ausspähen geheimer Daten zu verhindern. Die Verfälschung ist grundsätzlich bei allen Funktionen f möglich,

die ein lineares Verhalten gegenüber EXOR-Verknüpfungen zeigen. Bei nichtlinearen Funktionen g müssen die unverfälschten Daten verwendet werden. Es ist daher erforderlich, daß vor Anwendung der nichtlinearen Funktion g auf die Daten die Verfälschung durch eine EXOR-Verknüpfung der Daten mit dem Funktionswert f (Z) kompensiert wird. Dabei ist es unter Sicherheitsaspekten weniger kritisch, daß die nichtlinearen Funktionen g nur auf die unverfälschten Daten angewendet werden können, da diese nichtlinearen Funktionen g ohnehin wesentlich schwerer auszuspähen sind als die linearen Funktionen f. Das in Fig. 3 abgebildete Schema ist sowohl für gleiche Funktionen g bzw. gleiche Funktionen f als auch für jeweils unterschiedliche Funktionen anwendbar.

Mit dem in Fig. 3 dargestellten Schema wird erreicht, daß ein Ausspähen geheimer Daten im Zuge der Verarbeitung der Daten abc nahezu unmöglich wird. Da aber zudem bei der Bereitstellung der geheimen Schlüssel K1, K2 und K3 mit diesen Schlüsseln Operationen auszuführen sind, die ihrerseits Ziel eines Ausspähversuchs durch einen Angreifer sein könnten, empfiehlt es sich bei der Verarbeitung der Schlüssel entsprechende Sicherheitsvorkehrungen zu treffen. Eine Ausführungsform der Erfindung, bei der derartige Sicherheitsvorkehrungen vorgesehen sind, ist in Fig. 4 dargestellt.

Fig. 4 zeigt einen der Fig. 3 entsprechenden Ausschnitt eines Funktionsablaufs einer Chipkarte für eine Variante der Erfindung. Die Verarbeitung der Daten abc erfolgt in identischer Weise wie in Fig. 3 und wird daher im folgenden nicht nochmals erläutert. Im Gegensatz zur Fig 3 werden bei Fig. 4 in die Verknüpfungspunkte 7, 11 und 15, jedoch nicht die Schlüssel K1, K2 und K3 eingespeist. Stattdessen werden die verfälschten Schlüssel K1', K2' und K3' zusammen mit den für die Kompensation der Verfälschung benötigten Zufallszahlen Z1, Z2 und Z3 eingespeist, wobei bevorzugt erst die verfälsch-

ten Schlüssel und dann die Zufallszahlen eingespeist werden. Auf diese Weise wird sichergestellt, daß die richtigen Schlüssel K1, K2 und K3 überhaupt nicht in Erscheinung treten. Besonders vorteilhaft anwendbar ist diese Vorgehensweise bei Verschlüsselungsverfahren, bei denen die Schlüssel K1, K2 und K3 aus einem gemeinsamen Schlüssel K abgeleitet werden. In diesem Fall wird in der Chipkarte 1 der mit der Zufallszahl Z verfälschte Schlüssel K abgespeichert und es werden die durch Anwendung des Verfahrens zur Schlüsselableitung auf die Zufallszahl Z ermittelten Zufallszahlen Z1, Z2 und Z3 in der Chipkarte 1 abgespeichert. Diese Abspeicherung muß in einer sicheren Umgebung, beispielsweise in der Personalisierungsphase der Chipkarte 1 erfolgen.

Zur Durchführung des in Fig. 4 abgebildeten Funktionsschemas werden neben den abgespeicherten Daten noch die verfälschten abgeleiteten Schlüssel K1', K2' und K3' benötigt. Diese Schlüssel können dann, wenn sie benötigt werden, aus dem verfälschten Schlüssel K abgeleitet werden. Bei dieser Vorgehensweise werden keine Operationen mit dem echten Schlüssel K oder mit den echten abgeleiteten Schlüsseln K1, K2 und K3 durchgeführt, so daß ein Ausspähen dieser Schlüssel praktisch unmöglich ist. Da auch die abgeleiteten Zufallszahlen Z1, Z2 und Z3 bereits im Vorfeld ermittelt und in der Chipkarte 1 gespeichert wurden, werden auch mit diesen keine Operationen mehr ausgeführt, die von einem Angreifer ausgespäht werden könnten. Somit ist auch ein Zugang zu den echten abgeleiteten Schlüsseln K1, K2 und K3 durch Ausspähen der verfälschten abgeleiteten Schlüssel K1', K2' und K3' nicht möglich, da hierzu die abgeleiteten Zufallszahlen Z1, Z2 und Z3 benötigt werden.

Um die Sicherheit weiter zu erhöhen ist es auch möglich, für jede EXOR-Verknüpfung eine andere Zufallszahl Z zu verwenden, wobei dabei zu be-

achten ist, daß dann jeweils auch ein f (Z) zur Kompensation der Verfälschung vorhanden ist. In einer Ausführungsform werden sämtliche Zufallszahlen Z und Funktionswerte f (Z) im Speicher der Chipkarte gespeichert. Ebenso ist es aber auch möglich, jeweils nur eine geringe Anzahl von Zufallszahlen R und Funktionswerten f (Z) zu speichern und immer dann, wenn diese Werte benötigt werden, neue Zufallszahlen Z und Funktionswerte f (Z) durch EXOR-Verknüpfung oder eine andere geeignete Verknüpfung mehrerer gespeicherter Zufallszahlen Z und Funktionswerte F (Z) zu ermitteln. Dabei können die Zufallszahlen Z für die EXOR-Verknüpfung nach dem Zufallsprinzip aus der Menge der gespeicherten Zufallszahlen Z ausgewählt werden.

In einer weiteren Ausführungsform entfällt die Speicherung der Zufallszahlen Z und Funktionswerte f (Z), da diese jeweils bei Bedarf mittels geeigneter Generatoren erzeugt werden. Dabei ist es wichtig, daß der oder die Generatoren die Funktionswerte f (Z) nicht durch Anwendung der linearen Funktion f auf die Zufallszahl Z erzeugen sondern auf andere Art und Weise Paare von Zufallszahlen Z und Funktionswerten f (Z) erzeugt, da sonst durch Abhören der Anwendung der Funktion f auf die Zufallszahl Z möglicherweise diese Zufallszahl Z ausgespäht werden könnte und mit Hilfe dieser Information weitere geheime Daten ermittelt werden könnten.

Gemäß der Erfindung können grundsätzlich alle sicherheitsrelevanten Daten, beispielsweise auch Schlüssel, mit Hilfe weiterer Daten, wie beispielsweise Zufallszahlen, verfälscht werden und dann einer Weiterverarbeitung zugeführt werden. Dadurch wird erreicht, daß ein Angreifer, der diese Weiterverarbeitung ausspäht, nur wertlose, da verfälschte Daten ermitteln kann. Am Ende der Weiterverarbeitung wird die Verfälschung wieder rückgängig gemacht.

M 29.06.99

Patentansprüche

1. Datenträger mit einem Halbleiterchip (5) der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das in der Lage ist, eine Reihe von Operationen (f) auszuführen, wobei für die Ausführung der Operationen (f) Eingangsdaten benötigt werden und bei der Ausführung der Operationen (f) Ausgangsdaten erzeugt werden, dadurch **gekennzeichnet**, daß

die Eingangsdaten vor Ausführung einer oder mehrerer Operationen (f) durch Verknüpfung mit Hilfsdaten (Z) verfälscht werden,

die durch Ausführung der einen oder mehreren Operationen (f) ermittelten Ausgangsdaten mit einem Hilfsfunktionswert (f(Z)) verknüpft werden, um die Verfälschung der Eingangsdaten zu kompensieren,

wobei der Hilfsfunktionswert bereits vorab durch Ausführen der einen oder mehreren Operationen (f) mit den Hilfsdaten (Z) als Eingangsdaten in einer sicheren Umgebung ermittelt und ebenso wie die Hilfsdaten (Z) auf dem Datenträger gespeichert wurde.

2. Datenträger nach Anspruch 1, dadurch **gekennzeichnet**, daß die Verknüpfung mit den Hilfsfunktionswerten (f(Z)) zur Kompensation der Verfälschung spätestens unmittelbar vor Ausführung einer Operation (g) durchgeführt wird, die nichtlinear bezüglich der Verknüpfung ist, mit der die Verfälschung erzeugt wurde.

3. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Hilfsdaten (Z) variiert werden, wobei die jeweils zugehörigen Hilfsfunktionswerte (f(Z)) im Speicher des Datenträger gespeichert sind.

4. Datenträger nach Anspruch 3, dadurch gekennzeichnet, daß neue Hilfswerte (Z) und neue Hilfsfunktionswerte (f(Z)) durch Verknüpfung zweier oder mehrerer bestehender Hilfsdaten (Z) und Hilfsfunktionswerte (f(Z)) erzeugt werden.

5. Datenträger nach Anspruch 4, dadurch gekennzeichnet, daß die für die Verknüpfung vorgesehenen bestehenden Hilfsdaten (Z) und Hilfsfunktionswerte (f(Z)) jeweils zufallsbedingt ausgewählt werden.

6. Datenträger nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß mittels eines Generators Paare von Hilfsdaten (Z) und Hilfsfunktionswerten (f(Z)) erzeugt werden, ohne daß die Operation (f(Z)) auf die Hilfsdaten (Z) angewendet wird.

7. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß es sich bei den Hilfsdaten (Z) um eine Zufallszahl handelt.

8. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß es sich bei der Verknüpfung um eine EXOR-Verknüpfung handelt.

9. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß es sich bei dem Datenträger um eine Chipkarte handelt.

10. Verfahren zum Schutz von geheimen Daten, die als Eingangsdaten einer oder mehrerer Operationen dienen, dadurch **gekennzeichnet**, daß

---

die Eingangsdaten vor Ausführung der einen oder mehreren Operationen (f) durch Verknüpfung mit Hilfsdaten (Z) verfälscht werden,

die durch Ausführung der einen oder mehreren Operationen (f) ermittelten Ausgangsdaten mit einem Hilfsfunktionswert (f(Z)) verknüpft werden, um die Verfälschung der Eingangsdaten zu kompensieren,

wobei der Hilfsfunktionswert bereits vorab durch Ausführen der einen oder mehreren Operationen (f) mit den Hilfsdaten (Z) als Eingangsdaten in einer sicheren Umgebung ermittelt und ebenso wie die Hilfsdaten (Z) gespeichert wurde.

29.06.99

Zusammenfassung

Die Erfindung betrifft einen Datenträger (1) der einen Halbleiterchip (5) aufweist. Um zu verhindern, daß ein Angreifer aus abgehörten Signalverläufen des Chips (5) geheime Daten des Chips (5) ermittelt, werden die Eingangsdaten von sicherheitsrelevanten Operationen (f) vor der Ausführung der Operationen (f) durch Verknüpfung mit Hilfsdaten (Z) verfälscht. Nach Ausführung einer oder mehrerer der genannten Operationen (f) kann die Verfälschung durch Verknüpfung des mit den Operationen (f) ermittelten Ergebnisses mit einem Hilfsfunktionswert f(Z) kompensiert werden. Der Hilfsfunktionswert f(Z) wurde vorab durch Ausführung der genannten Operationen (f) mit den Hilfsdaten (Z) in einer sicheren Umgebung ermittelt und ebenso wie die Hilfsdaten (Z) selbst auf den Datenträger gespeichert.

(Fig. 1)

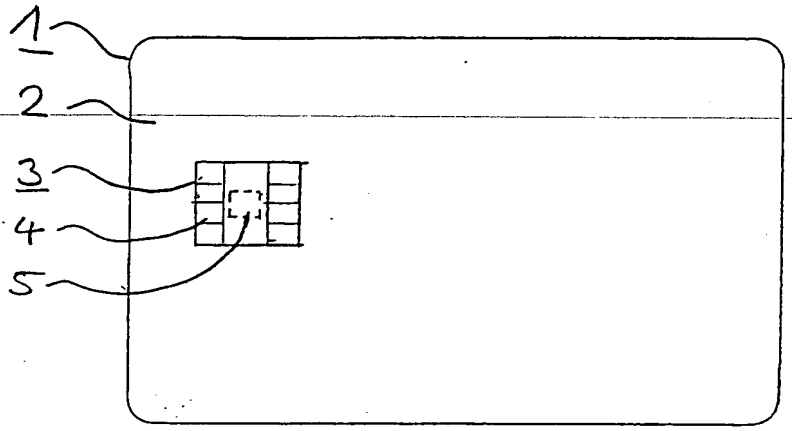

Fig. 1

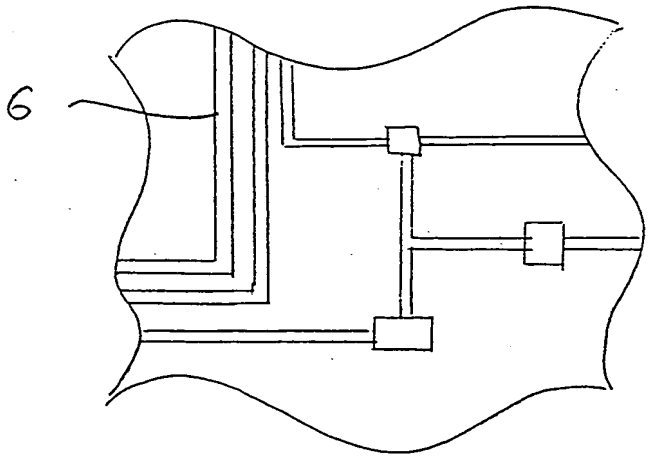

Fig. 2

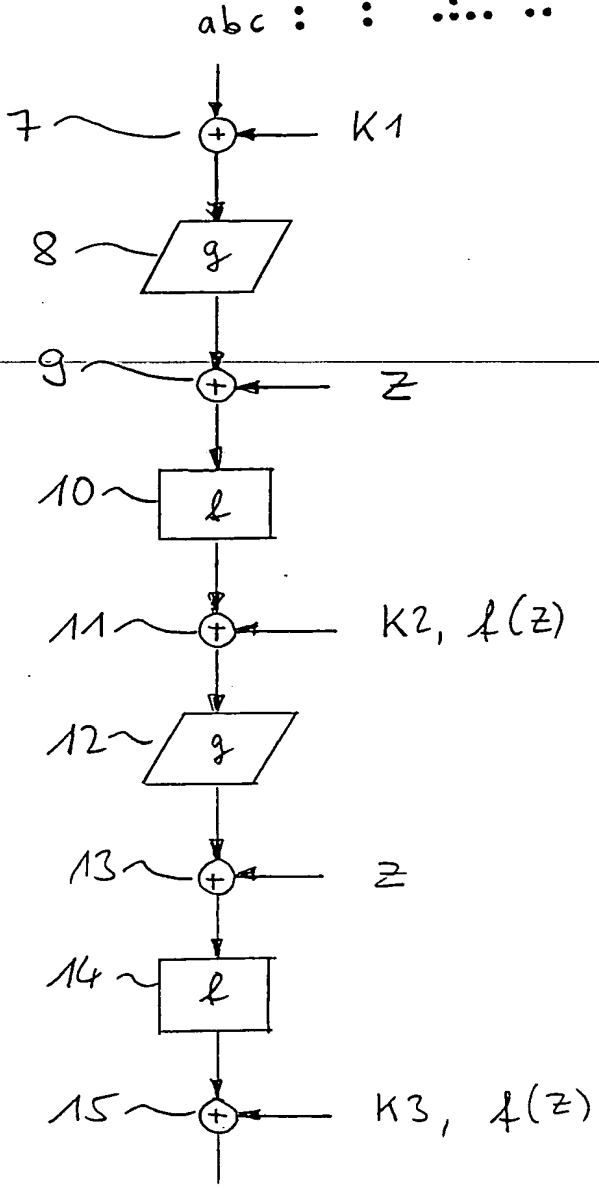

Fig. 3

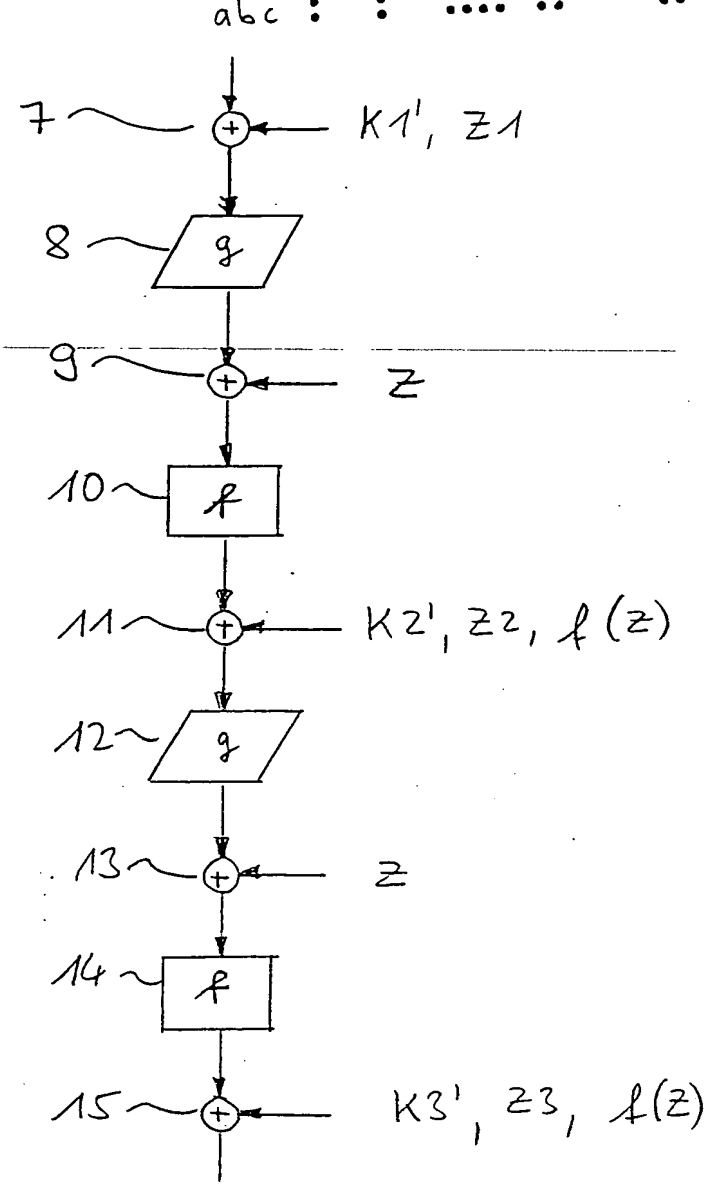

Fig. 4

M 29.06.99

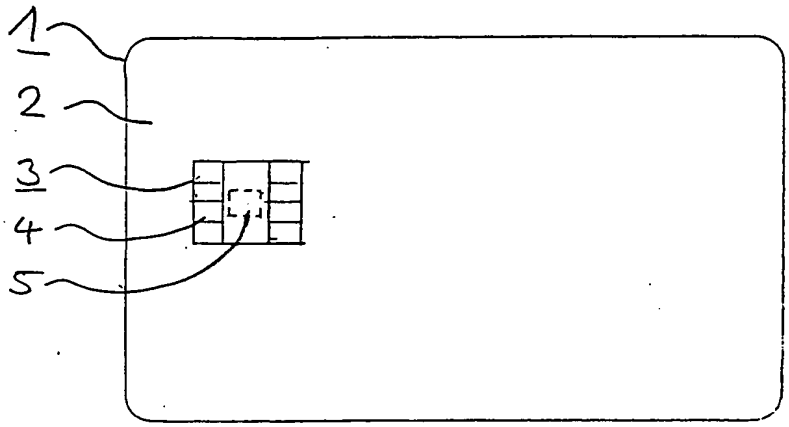

Fig. 1